

VISIT...

LANZAROTE
Caliente.COM

21

Security Analysis

Nouredine Hadjsaid

*Institut National Polytechnique de
Grenoble (INPG)*

21.1	Definition	21-2
21.2	Time Frames for Security-Related Decision	21-2
21.3	Models	21-3
21.4	Determinist vs. Probabilistic	21-5
	Security under Deregulation	
Appendix A		21-5
Appendix B		21-6

The power system as a single entity is considered the most complex system ever built. It consists of various equipment with different levels of sophistication, complex and nonlinear loads, various generations with a wide variety of dynamic responses, a large-scale protection system, a wide-area communication network, and numerous control devices and control centers. This equipment is connected with a large network (transformers, transmission lines) where a significant amount of energy transfer often occurs. This system, in addition to the assurance of good operation of its various equipment, is characterized by an important and simple rule: electricity should be delivered to where it is required in due time and with appropriate features such as frequency and voltage quality. Environmental constraints, the high cost of transmission investments and low/long capital recovery, and the willing of utilities to optimize their network for more cost effectiveness makes it very difficult to expand or oversize power systems. These constraints have pushed power systems to be operated close to their technical limits, thus reducing security margins.

On the other hand, power systems are continuously subjected to random and various disturbances that may, under certain circumstances, lead to inappropriate or unacceptable operation and system conditions. These effects may include cascading outages, system separation, widespread outages, violation of emergency limits of line current, bus voltages, system frequency, and loss of synchronism (Debs and Benson, 1975). Furthermore, despite advanced supervisory control and data acquisition systems that help the operator to control system equipment (circuit breakers, on-line tap changers, compensation and control devices, etc.), changes can occur so fast that the operator may not have enough time to ensure system security. Hence, it is important for the operator not only to maintain the state of the system within acceptable and secure operating conditions but also to integrate preventive functions. These functions should allow him enough time to optimize his system (reduction of the probability of occurrence of abnormal or critical situations) and to ensure recovery of a safe and secure situation.

Even though for small-scale systems the operator may eventually, on the basis of his experience, prevent the consequences of most common outages and determine the appropriate means to restore a secure state, this is almost impossible for large systems. It is therefore essential for operators to have at their disposal, efficient tools capable of handling a systematic security analysis. This can be achieved through the diagnosis of all contingencies that may have serious consequences. This is the concern of **security analysis**.

The term contingency is related to the possibility of losing any component of the system, whether it is a transmission line, a transformer, or a generator. Another important event that may be included in this

definition concerns busbar faults (bus split). This kind of event is, however, considered rare but with (serious) dangerous consequences. Most power systems are characterized by the well-known $N - 1$ security rules where N is the total number of system components. This rule is the basic requirement for the planning stage where the system should be designed in order to withstand (or to remain in a normal state) any single contingency. Some systems also consider the possibility of $N - 2/k$ (k is the number of contingencies), but mostly for selected and specific cases.

21.1 Definition

The term security as defined by NERC (1997) is the ability of the electric systems to withstand sudden disturbance such as electric short-circuits or unanticipated loss of system elements. (See [Appendix A](#)).

Security analysis is usually handled for two time frames: static and dynamic. For the static analysis, only a “fixed picture” or a snapshot of the network is considered. The system is supposed to have passed the transient period successfully or be dynamically stable. Therefore, the monitored variables are line flows and bus voltages. Hence, all voltages should be within a predefined secure range, usually around $\pm 5\%$ of nominal voltage (for some systems, such as distribution networks, the range may be wider). In fact, if bus voltages drop below a certain level, there will be a risk of voltage collapse in addition to high losses. On the other hand, if bus voltages are too high compared to nominal values, there will be equipment degradation or damage. Furthermore, overload of transmission lines may be followed by unpredictable line tripping that accelerates the degradation of the voltage profile.

Line flows are related to circuit overload (lines and transformers) and should keep below a maximum limit, usually settled according to line thermal limits. The dynamic security is related to loss of synchronism (transient stability) and oscillatory swings or dynamic instability. In that case the evolution of essential variables are monitored based upon a required time frame (transient period).

Normally, system security is analyzed differently whether it is considered for planning studies or for monitoring and operational purposes. The difference comes from the type of action that should be initiated in case of expected harmful contingencies. However, for both stages, all variables should remain within the bounded domain defining or determining system normal state (Fink, 1978).

21.2 Time Frames for Security-Related Decision

There are generally three different time frames for security-related decisions. In operations, the decision-maker is the operator, who must continuously monitor and operate his system economically in such a way that the normal state is appropriately preserved (maintained). For this purpose, he has specific tools for diagnosing his system and operating rules that allow the required decisions to be made in due time. In operational planning, the operating rules are developed recognizing that the bases for the decision are reliability/security criteria specifying minimum operating requirements, which define acceptable performance for the credible contingencies. In facility planning, the planner must determine the best way to reinforce the transmission system, based on reliability/security criteria for system design, which generally adhere to the same disturbance-performance criteria specified by minimum operating requirements.

One may think that since these systems are designed to operate “normally” or in “a secure state” for a given security rule ($N - k$), there is nothing to worry about during operations. The problem is that, during the planning stage and for a set of given economical constraints, a number of assumptions are made for operating conditions that concern topology, generation, and consumption. Since there may be several years between the planning stage and the operations, the uncertainties in the system’s security may be very significant. Therefore, security analysis is supplemented by operational planning and operations studies.

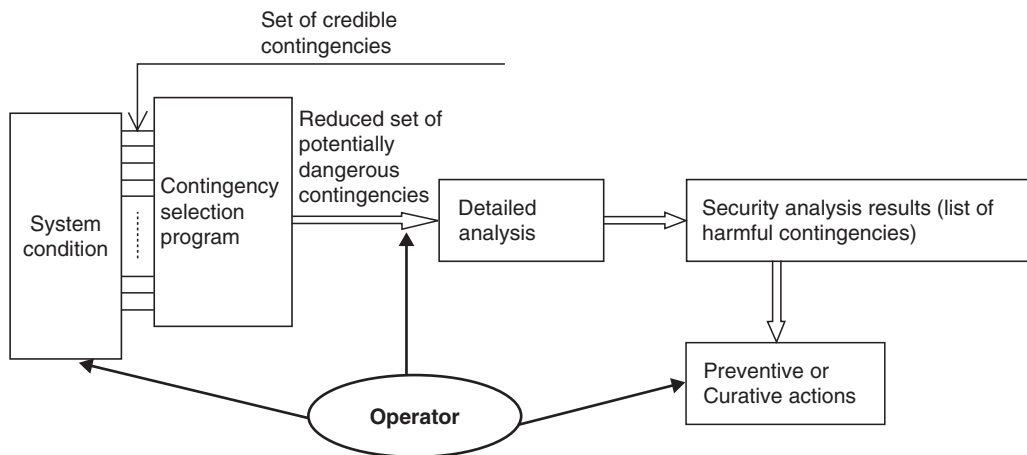


FIGURE 21.1 Contingency analysis procedure.

The decision following any security analysis can be placed in one of two categories: preventive or corrective actions. For corrective actions, once a contingency or an event is determined as potentially dangerous, the operator should be confident that in case of that event, he will be able to correct the system by means of appropriate actions on system conditions (generation, load, topology) in order to keep the system in a normal state and even away from the insecure region. The operator should also prepare a set of preventive actions that may correct the effect of the expected dangerous event.

In operations, the main constraint is the time required for the analysis of the system's state and for the required decision to be made following the security analysis results. The security analysis program should be able to handle all possible contingencies, usually on the $N - 1$ basis or on specific $N - 2$. For most utilities, the total time window considered for this task is between 10 min and 30 min. Actually for this time window, the system's state is considered as constant or quasi-constant allowing the analysis to be valid within this time frame. This means that changes in generation or in consumption are considered as negligible.

For large systems, this time frame is too short even with very powerful computers. Since it is known that only a small number of contingencies may really cause system violations, it has been realized that it is not necessary to perform a detailed analysis on all possible contingencies, which may be on the order of thousands. For this purpose, the operator may use his engineering judgment to select those contingencies that are most likely to cause system violation. This procedure has been used (and is still in use) for many years in many control centers around the world. However, as system conditions are characterized by numerous uncertainties, this approach may not be very efficient especially for large systems.

The concept of contingency selection has arisen in order to reduce the list of all possible contingencies to only the potentially harmful. The selection process should be very fast and accurate enough to identify dangerous cases (Hadjsaid, 1992). This process has existed for many years, and still is a major issue in all security studies for operations whether for static or dynamic and transient purposes.

21.3 Models

The static security analysis is mainly based on load flow equations. Usually, active/angle and reactive/voltage problems are viewed as decoupled. The active/angle subproblem is expressed as (Stott and Alsac, 1974):

$$\Delta\theta = [dP/d\theta]^{-1}\Delta P \quad (21.1)$$

where $\Delta\theta$ is a vector of angular changes with a dimension of $N_b - 1$ (N_b = number of buses), ΔP a vector of active injection changes ($N_b - 1$) and $[dP/d\theta]$ is a part of the Jacobian matrix. In the DC approach, this Jacobian is approximated by the B' (susceptance) matrix representing the imaginary part of the Y_{bus} matrix. This expression is used to calculate the updated angles following a loss of any system component. With appropriate numerical techniques, it is straightforward to update only necessary elements of the equation. Once the angles are calculated, the power flows of all lines can be deducted. Hence, it is possible to check for line limit violation.

Another approach that has been, and still is used in many utilities for assessing the impact of any contingency on line flows is known as shift factors. The principle used recognizes that the outage of any line will result in a redistribution of the power previously flowing through this line on all the remaining lines. This distribution is mainly affected by the topology of the network. Hence, the power flow of any line ij following an outage of line km can be expressed as (Galiana, 1984) (see Appendix B for more details):

$$P_{ij/km} = P_{ij} + \alpha_{ij/km} * P_{km} \quad (21.2)$$

where

$P_{ij/km}$ is the active power flow on line ij after the outage of line km

P_{ij} , P_{km} is the active power previously flowing respectively on line ij and km (before the outage)

$\alpha_{ij/km}$ is the shift factor for line ij following the outage of line km

Equation (21.2) shows that the power flow of line ij ($P_{ij/km}$) when line km is tripped, is determined as the initial power flow on line ij (P_{ij}) before the outage of line km plus a proportion of the power flow previously flowing on line km . This proportion is defined by the terms $\alpha_{ij/km} * P_{km}$.

The shift factors are determined in a matrix form. The important features of these factors are the simplicity of computing and their dependency on network topology. Therefore, if the topology does not change, the factors remain constant for any operating point. The main drawback of these factors is that they are determined on the basis of DC approximation and the shift factor matrix should be updated for any change in the topology. In addition, for some complex disturbances such as bus split, updating these factors becomes a complicated task.

A similar method based on reactive power shift factors has been developed. Interested readers may refer to Ilic-Spong and Phadke (1986) and Taylor and Maahs (1991) for more details.

The reactive/voltage subproblem can be viewed as (Stott and Alsac, 1974):

$$\Delta V = [dQ/dV]^{-1} \Delta Q \quad (21.3)$$

where

ΔV is the vector of voltages change ($N_b - N_g$, N_g is the number of generators)

ΔQ is the vector of reactive power injections change ($N_b - N_g$, N_g is the number of generators)

$[dQ/dV]$ is the Jacobean submatrix

In the well-known FDLF (Fast Decoupled Load Flow) model (Stott and Alsac, 1974), the Jacobian submatrix is replaced by the B'' (susceptance) matrix representing the imaginary part of the Y_{bus} matrix with a dimension of $N_b - N_g$, where N_g is the number of voltage regulated (generator) buses. In addition, the vector ΔQ is replaced by $\Delta Q/V$.

Once bus voltages are updated to account for the outage, the limit violations are checked and the contingency effects on bus voltages can be assessed.

The most common framework for the contingency analysis is to use approximate models for the selection process, such as the DC model, and use the AC power flow model for the evaluation of the actual impact of the given contingency on line flows and bus voltages.

Concerning the dynamic security analysis, the framework is similar to the one in static analysis in terms of selection and evaluation. The selection process uses simplified models, such as Transient Energy Functions (TEF), and the evaluation one uses detailed assessing tools such as time domain simulations.

The fact that the dynamic aspect is more related to transient/dynamic stability technique makes the process much more complicated than for the static problem. In fact, in addition to the number of contingencies to be analyzed, each analysis will require detailed stability calculations with an appropriate network and system component model such as the generator model (park, saturation, etc.), exciter (AVR: Automatic Voltage Regulator; PSS: Power System Stabilizer), governor (nuclear, thermal, hydro-electric, etc.), or loads (non-linear, constant power characteristics, etc.). In addition, integration and numerical solutions are an important aspect for these analyses.

21.4 Determinist vs. Probabilistic

The basic requirement for security analysis is to assess the impact of any possible contingency on system performance. For the purpose of setting planning and operating rules that will enable the system to be operated in a secure manner, it is necessary to consider all credible contingencies, different network configurations, and different operating points for given performance criteria. Hence, in the deterministic approach, these assessments may involve a large number of computer simulations even if there is a selection process at each stage of the analysis. The decision in that case is founded on the requirement that each outage event in a specified list, the contingency set, results in system performance that satisfies the criteria of the chosen performance evaluation (Fink and Carlsen, 1978). To handle these assessments for all possible situations by an exhaustive study is generally not reasonable. Since the resulting security rules may lead to the settlement and schedule of investment needs as well as operating rules, it is important to optimize the economical impact of security measures that have to be taken in order to be sure that there is no unnecessary or unjustified investment or operating costs. This has been the case for many years, since the emphasis was on the most severe, credible event leading to overly conservative solutions.

One way to deal with this problem is the concept of the probability of occurrence (contingencies) in the early stage of security analysis. This can be jointly used with a statistical approach (Schlumberger et al., 1999) that allows the generation of appropriate scenarios in order to fit more with the reality of the power system from the technical point of view as well as from the economical point view.

21.4.1 Security under Deregulation

With deregulation, the power industry has pointed out the necessity to optimize the operations of their systems leading to less investment in new facilities and pushing the system to be exploited closer to its limits. Furthermore, the open access has resulted in increased power exchanges over the interconnections. In some utilities, the number of transactions previously processed in one year is now managed in one day. These increased transactions and power exchanges have resulted in increased parallel flows leading to unpredictable loading conditions or voltage problems. A significant number of these transactions are non-firm and volatile. Hence, the security can no longer be handled on a zonal basis but rather on large interconnected systems.

Appendix A

The current NERC basic reliability requirement from NERC Policy 2- transmission (Pope, 1999) is:

Standards

1. Basic reliability requirement regarding single contingencies: All control areas shall operate so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single contingency.
 - 1.1 Multiple contingencies: Multiple outages of credible nature, as specified by regional policy, shall also be examined and, when practical, the control areas shall operate to

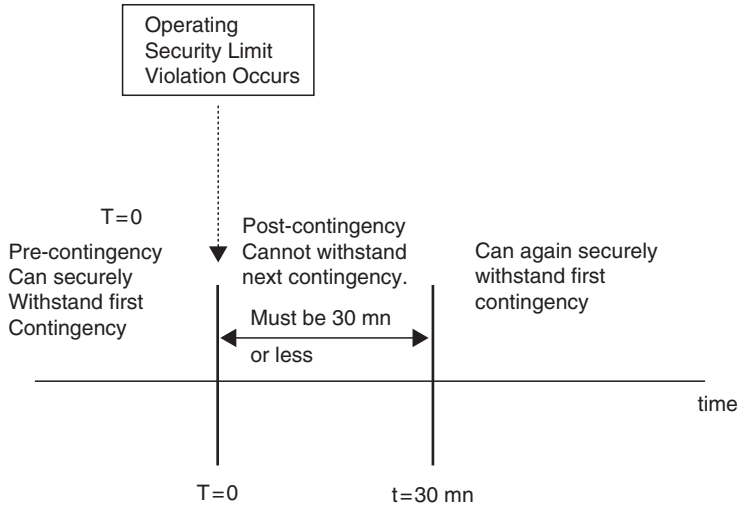


FIGURE 21.2 Current NERC basic reliability requirement. (Pope, J.W., Transmission Reliability under Restructuring, in *Proceedings of IEEE SM 1999*, Edmonton, Alberta, Canada, 162–166, July 18–22, 1999. With permission.)

protect against instability, uncontrolled separation, or cascading outages resulting from these multiple outages.

1.2 Operating security limits: Define the acceptable operating boundaries

2. Return from Operating security limit violation: Following a contingency or other event that results in an operating security limit violation, the control area shall return its transmission system to within operating security limits soon as possible, but no longer than 30 minutes.

Appendix B

Shift factor derivation (Galiana, 1984)

Consider a DC load flow for a base case:

$$[B']\underline{\theta} = \underline{P}$$

where

$\underline{\theta}$ is the vector of phase angles for the base case

$[B']$ is the susceptance matrix for the base case

$\underline{P}$ is the vector of active injections for the base case

Suppose that the admittance of line jk is reduced by ΔY_{jk} and the vector $\Delta \underline{P}$ is unchanged, then:

$$\left[[B'] - \Delta Y_{jk} \underline{e}_{jk} \underline{e}_{jk}^T \right] \underline{\theta} = \underline{P}$$

where $\underline{e}_{jk}$ is the vector $(Nb - 1)$ containing 1 in the position j , -1 in the position k and 0 elsewhere
 T is the Transpose

Now we can compute the power flow on an arbitrary line lm when line jk is outaged:

$$\begin{aligned} P_{lm/jk} &= Y_{lm}(\theta_l - \theta_m) = Y_{lm} \underline{e}_{lm}^T \underline{\theta} \\ &= Y_{lm} \underline{e}_{lm}^T \left[[B'] - \Delta Y_{jk} \underline{e}_{jk} \underline{e}_{jk}^T \right]^{-1} \underline{P} \end{aligned}$$

By using the matrix inversion lemma, we can compute:

$$P_{lm/jk} = Y_{lm} e_{lm}^T \left[[B'] + \left([B']^{-1} e_{jk} e_{jk}^T [B']^{-1} \right) / \left((\Delta Y_{jk}) - 1 - e_{jk}^T [B']^{-1} e_{jk} \right) \right] P$$

Finally:

$$P_{lm/jk} = P_{lm} + \alpha_{jk/jk} * P_{jk}$$

where

$$\alpha_{jk/jk} = Y_{lm} * \left(\Delta Y_{jk} / Y_{jk} \right) * \left(e_{lm}^T [B']^{-1} e_{jk} \right) / \left(1 - \Delta Y_{jk} e_{jk}^T [B']^{-1} e_{jk} \right)$$

References

- Debs, A.S. and Benson, A.R., Security Assessment of Power Systems, in *System Engineering for Power: Status and Prospects*, Henniker, New Hampshire, 144–178, Aug. 17–22, 1975.
- Fink, L. and Carlsen, K., Operating Under Stress and Strain, *IEEE Spectrum*, 15, 48–53, March, 1978.
- Galiana, F.D., Bound estimates of the severity of line outages in power system contingency analysis and ranking, *IEEE Trans. on Power Appar. and Syst.*, PAS-103(9), 2612–2624, September 1984.
- Hadjsaid, N., Benahmed, B., Fandino, J., Sabonnadiere, J.-Cl., and Nerin, G., Fast contingency screening for voltage-reactive considerations in security analysis, *IEEE Winter Meeting*, 1992 WM 185-9 PWRs.
- Illic-Spong, M. and Phadke, A., Redistribution of reactive power flow in contingency studies, *IEEE Trans. on Power Syst.*, PWRs-1(3), 266–275, August 1986.
- McCaulley, J.D., Vittal, V., and Abi-Samra, N., An overview of risk based security assessment, in *Proceedings of IEEE SM'99*, Edmonton, Alberta, Canada, 173–178, July 18–22, 1999.
- The North American Reliability Council, NERC Planning Standards, approved by NERC Board of Trustees, September, 1997.
- Pope, J.W., Transmission reliability under restructuring, in *Proceedings of IEEE SM'99*, Edmonton, Alberta, Canada, 162–166, July 18–22, 1999.
- Schlumberger, Y., Lebrevelec, C., and De Pasquale, M., Power system security analysis: New approaches used at EDF, in *Proceedings of IEEE SM'99*, Edmonton, Alberta, Canada, 147–151, July 18–22, 1999.
- Stott, B. and Alsac, O., Fast decoupled load flow, *IEEE Trans. on Power Appar. and Syst.*, PAS-93, pp. 859–869, May/June 1974.
- Taylor, D.G. and Maahs, L.J., A reactive contingency analysis algorithm using MW and MVAR distribution factors, *IEEE Trans. on Power Syst.*, 6, 349–355, February 1991.

